

UNCLASSIFIED

The Fifth User January 28

Project VENONA is now well known publicly. VENONA refers to Soviet espionage messages that were solved in part or in whole by the U.S. cryptologic services. The Soviet cryptosystem was based on a one-time pad that was misused, and therefore vulnerable to American cryptanalysts. The cryptosystem was used by the USSR's diplomatic service and its office for acquiring lend-lease equipment from the United States during World War II. This Soviet system was in use from 1941 to 1945, but was not solved until the late 1940s, after the war, and the most usable product based on the decrypts was issued in the 1950s.

In addition, the cryptosystem was used by the espionage organization best known as the KGB. When people think of VENONA decrypts, they most often mean KGB communications. However, there were other users of the flawed system.

The fifth user of the cryptosystem was known in English as GRU-Naval. Its communications referred to espionage operations controlled by the Naval Intelligence headquarters in Moscow. The senior representative in the U.S. was Captain, later Commodore, I. A. Egorichev, the USSR's naval attaché in Washington. During his career he had commanded a destroyer in the Soviet's Baltic fleet, and had served as naval attaché in Tokyo. In addition to legal duties in his overt position, Captain Egorichev conducted intelligence activities against the United States.

The GRU-Naval cryptosystem worked in the same way the KGB and GRU systems did. Message text was encoded into numbers from a codebook, then the numbers were superenciphered with numbers from a one-time pad. As with the others users, unknown to them, some pages from the pads had been printed twice; this is what made them vulnerable to U.S. cryptanalysts.

But, the GRU-Naval messages had some key differences from the VENONA messages sent by the KGB or the Army's GRU. First, many of the individual messages do not refer to intelligence activities. Egorichev, as attaché, was the Russian Navy's official representative to the U.S. government, and a significant

UNCLASSIFIED

UNCLASSIFIED

number of the messages dealt with his legitimate activities, which, with a war on, were considerable. Second, the GRU-Naval messages used very few covernames for individuals; instead, the names often were spelled out, using a spell table within the GRU-Naval codebook. In addition, a block of blank numbers in the back of the code book were set aside for names, which were inked in when a name was used frequently in the traffic. A few individuals were mentioned both by their true name and by the numerical designation from the code book.

Many of the messages related to Captain Egorichev's attaché duties simply report information on U.S. Navy activities worldwide, based on briefings given by American officers to the Washington diplomatic corps. Other messages report on the daily business that were conducted with his American counterparts.

Egorichev reported on attempts by U.S. intelligence organizations to place Russian-speaking personnel under cover in ports where Soviet ships docked. According to a text from April 18, 1943, these covert agents were seeking to undermine the morale of Soviet sailors, getting them drunk to solicit information or spread dissatisfaction among them.

The GRU-Naval communications discussed some covert intelligence activities. For example, they collected information from an agent who did have a codename, CARTER. CARTER was an electrical engineer working at the RCA Laboratory in Princeton, New Jersey; he passed information to the Soviets about navigational radar being designed for U.S. Army Air Force bombers.

Although the percentage of GRU-Naval traffic exploited was high, it was less useful. Most of the decrypted messages related directly to wartime situations, and did not relate to individuals or operations that continued into the postwar period, as the KGB and GRU decrypts did. Nevertheless, the GRU-Naval portion of the VENONA project did provide an insight into Soviet intelligence activities during the time they were America's allies and before the Cold War began.

UNCLASSIFIED